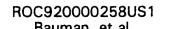
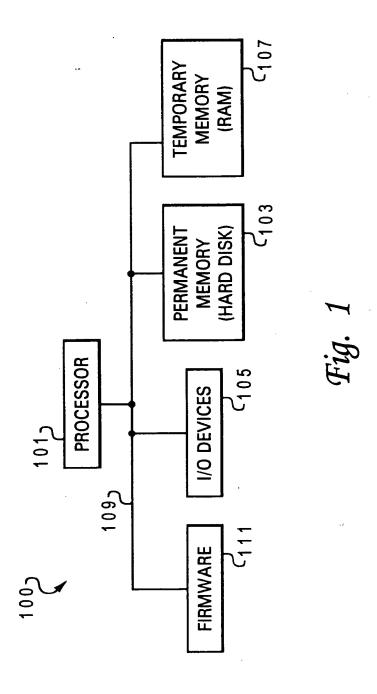
MAR 1 8 2005



ROC920000258US1
Bauman, et al.
System Console Device Authentication in a Network Environment

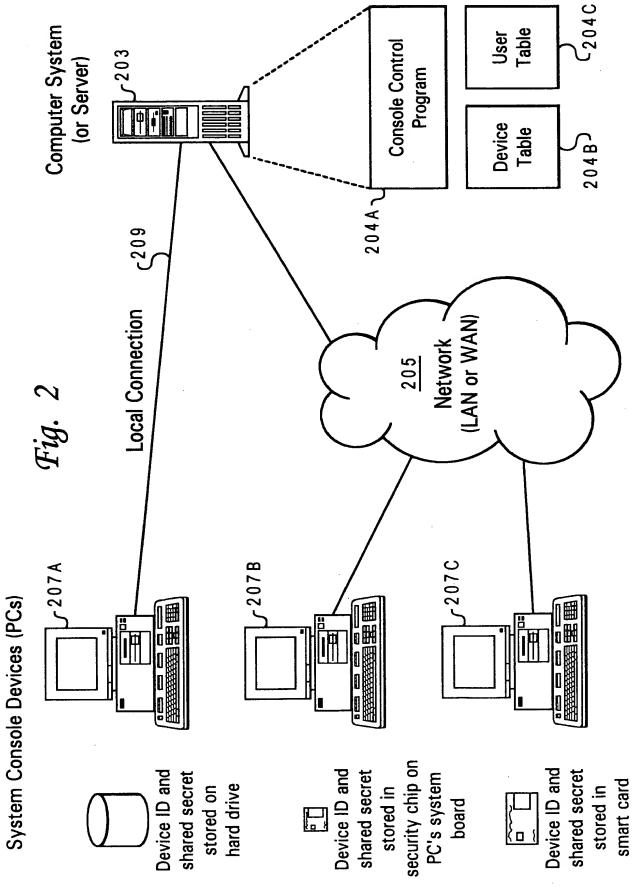
1/9



# MAR 1 8 2005

## ROC920000258US1 Bauman, et al. System Console Device Authentication in a Network Environment

2/9



3/9

Derive K<sub>U</sub>

Set  $H(P_D) = H(K_D)$ Derive K<sub>D</sub>

Console session flow

Op Console PC

301

**0S/400** 

2) Use PKCS-5 to encrypt P<sub>D</sub> with P<sub>A</sub> 1) Prompt for  $I_D$ ,  $P_D$ ,  $P_A$ ,  $I_{Ux}$ ,  $P_{Ux}$ Prompt for  $I_D$  ,  $P_A$  ,  $I_{Ux}$  ,  $P_{Ux}$ Setup wizard -Normal flow -

Device EKE flow with H(P<sub>D</sub>)

 $I_{U1} = 111111111, H(P_{U1}) = H(11111111)$  $I_{U2} = 2222222$ ,  $H(P_{U2}) = H(2222222)$ 

 $I_D = QCONSOLE, H(P_D) = H(QCONSOLE)$  $I_{U3} = QSECOFR$ ,  $H(P_{U3}) = H(QSECOFR)$ 

Shipped with:

User EKE flow with H(P<sub>U</sub>)

Set  $P_D = K_D$  if first use of  $P_D$ 

Derive K<sub>U</sub>

Derive K<sub>D</sub>

Secure console session Encrypted with Ku

> P<sub>D</sub> = Device shared secret  $A_A = Access passphrase$

I<sub>D</sub> = Device identifier

 $K_D = Device session key$ 

 $K_U$  = User session key

R = Random number H(x) = Hash of x

 $P_{UX} = User passphrase$ 

 $I_{Ux} = User ID$ 

NOTE: The first console session uses the well known shipped device identifier and user ID to access the iSeries. The device Therefore, the genesis device essentially "gets in free." passphrase is modified in the initial flow ( $P_D = K_D$ ).

Fig. 3A



4/9

- Generate of parametric g and gMake g, p constants Server EKE - Make g and p constants in server and client EKE code Generate DH parameters g and p Make g, p constants Client EKE

303

Device ID, H(P<sub>D</sub>)[public-info]

Generate R and do DH Phase

Send -->

Generate R and do DH Phase 1
Generate challenge B
Derive K from DH Phase 2
<-- Send (Phase 1 public-info), K[challenge B]

Derive K from DH Phase 2 Generate challenge A Send --> K[H(challenge A, challenge B)]

K[challenge A, challenge B]

Authenticate user A

<-- Send

Authenticate server B

NOTE: The challenge strings must be a different length than the encryption block. Refer to BSAFE Reference Manual for description of DH Phase 1 & 2.



5/9

Control Program EKE\_Handshake Server EKE (version, key strength) **EKE** negotiation **EKE Interface** 305

**EKE Interface** 

Console

Client EKE

EKE negotiation (version, key strength)

EKE Handshake

**EKE** negotiation response

Generate device R and do DH Phase 1

EKE parms, H(P<sub>D</sub>)[public-info] Device ID,

Generate device R and do DH Phase

Generate device challenge B Derive K<sub>D</sub> from DH Phase 2

H(P<sub>D</sub>)[public-info], K<sub>D</sub>[challenge B]

Derive K<sub>D</sub> from DH Phase 2

Generate device challenge A

K<sub>D</sub>[H(challenge A, challenge B)]

K<sub>D</sub>[challenge A, challenge B]

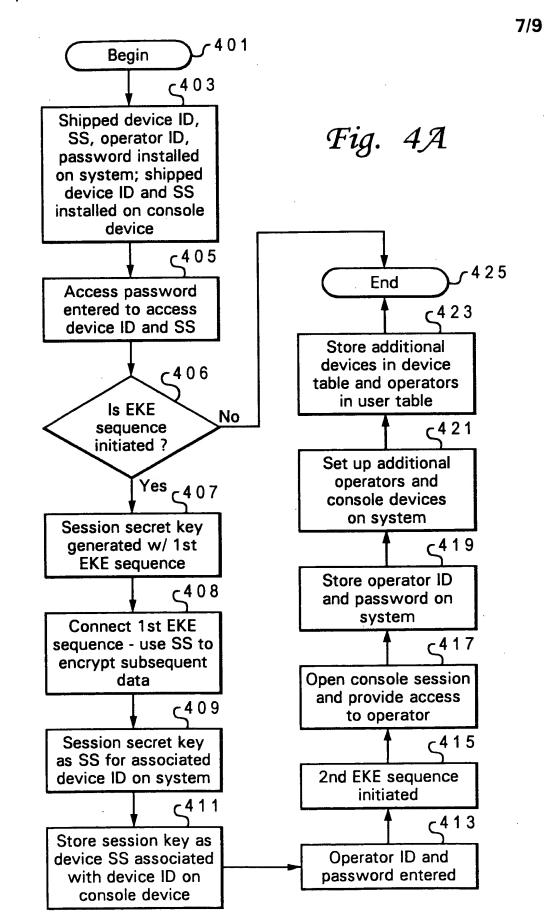
Authenticate Console device

Authenticate server

Pass 1 for device complete, begin Pass 2 for user...



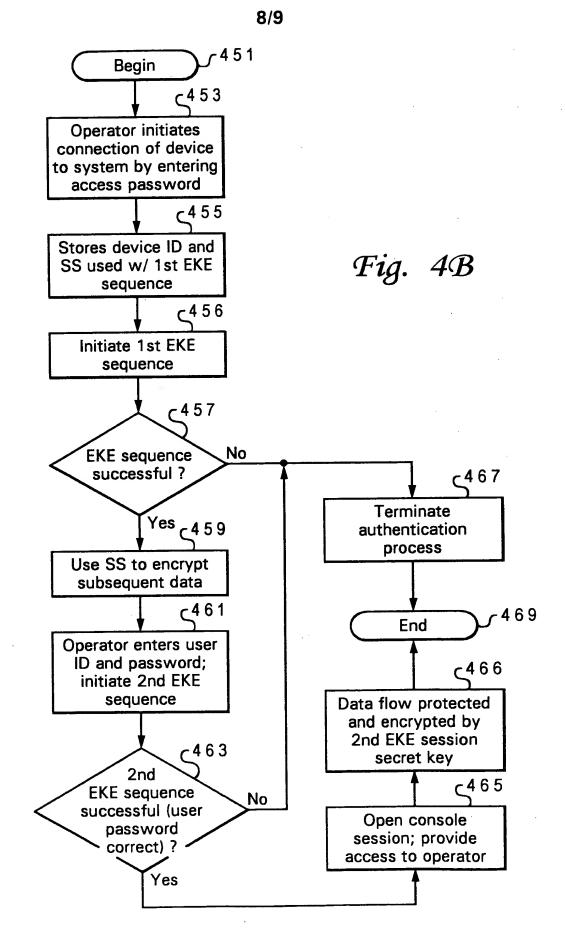
6/9 Control Program EKE\_Read Process data EKE\_Write Generate user R and do DH Phase 1 Server EKE Derive K<sub>U</sub> from DH Phase 2 Generate user challenge B Authenticate user **EKE Interface** H(P<sub>U</sub>)[public-info], K<sub>U</sub>[challenge B] K<sub>U</sub>[H(challenge A, challenge B)] Fig. 3D K $_{
m U}$ [challenge A, challenge B] User ID, H(P<sub>U</sub>)[public-info] K<sub>U</sub>[console data] K<sub>U</sub>[console data] 307 Generate user R and do DH Phase Derive K<sub>U</sub> from DH Phase 2 Generate user challenge A Authenticate server **EKE Interface** Client EKE Console



## MAR 1 8 2005

#### ROC920000258US1 Bauman, et al.

System Console Device Authentication in a Network Environment





9/9

Device Identifier | Hashed shared H(shared H(shared secret) secret) **Device Table** secret Server **QCONSOLE DEVICE2** 

Client Device (PC)  $\zeta^{501}$ 

(513 password Hashed User Table

H(password) H(password) H(password) H(password) 222222 **QSECOFR** dentifier **OSRV** User

shared secret)

Hash (device

Server2

identifier,

shared secret)

identifier,

Hash (device

Connection

Server

Server1

Fig. 5A